Audit Report

OFFICE OF THE INSPECTOR GENERAL

FOLLOWUP AUDIT OF CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE AND OTHER GENERAL CONTROLS FOR COMPUTER SYSTEMS SUPPORTING THE DEFENSE FINANCE AND ACCOUNTING SERVICE

Report No. 96-053 January 3, 1996

Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8939 (DSN 664-8939) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

Inspector General, Department of Defense
OAIG-AUD (ATTN: APTS Audit Suggestions)
400 Army Navy Drive (Room 801)
Arlington, Virginia 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@DODIG.OSD.MIL; or by writing the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ACID	Accessor Identifier
AFAA	Air Force Audit Agency
APF	Authorized Program Facility
DFAS	Defense Finance and Accounting Service
DIPC	Defense Information Processing Center
DISA	Defense Information Systems Agency
DLA-DSDC	Defense Logistics Agency, Defense Systems Design Center
DMC	Defense Megacenter
FSA	Financial Systems Activity
IBM	International Business Machines Corporation
IG	Inspector General
JES2	Job Entry Subsystem 2
MCCTA	Marine Corps Computer and Telecommunications Activity
MVS	Multiple Virtual Storage
PPT	Program Properties Table
SVC	Supervisor Call
WESTHEM	Western Hemisphere

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

January 3, 1996

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Audit Report on the Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service (Report No. 96-053)

We are providing this report for review and comment. We performed the audit in response to a request from the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). We considered management comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be promptly resolved. Comments from the Defense Information Systems Agency were generally responsive, but specific comments were not provided on all of the recommendations. Therefore, additional comments are requested by February 5, 1996, as indicated at the end of Finding B in Part I of the report.

We appreciate the courtesies extended to our audit staff. Questions about the audit should be directed to Mr. David C. Funk, Audit Program Director, at (303) 676-7445 (DSN 926-7445), or Mr. W. Andy Cooley, Audit Project Manager, at (303) 676-7393 (DSN 926-7393). See Appendix G for the report distribution. The audit team members are listed inside the back cover.

David Steensma
for
Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 96-053 January 3, 1996
(Project NO. 5FD-5026)

Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service

Executive Summary

Introduction. This is the third in a series of followup audits made to evaluate the corrective actions taken by the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Defense Logistics Agency in response to prior audits of computer security and other general controls. This audit focused on actions by the Defense Information Systems Agency, Western Hemisphere Defense megacenters in Denver, Colorado, and St. Louis, Missouri, to correct security problems with computer systems that migrated from the former Defense Information Processing Centers in Indianapolis, Indiana, and Kansas City, Missouri, and from the Marine Corps Computer and Telecommunications Activity in Quantico, Virginia. The followup audits were requested by the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence).

Audit Objectives. Our objective was to determine whether corrective actions taken or planned by the two Defense megacenters to improve computer security adequately responded to the recommendations made in two prior reports:

o Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992, and

o Report No. 94-065, same title, March 24, 1994.

The audit also evaluated the effectiveness of applicable management controls.

Audit Results. The two Defense megacenters made commendable efforts to implement 22 of the 25 prior audit recommendations. The Defense Megacenter, St. Louis, Missouri, adequately implemented all of the prior recommendations applicable to the systems that migrated to it. At the Defense Megacenter, Denver, Colorado, the planned corrective actions on the remaining three recommendations were considered adequate, although incomplete. A new security software problem was identified during the audit, requiring corrective action by the Defense Information Systems Agency, Western Hemisphere, Fort Ritchie, Maryland.

Due to their sensitive nature, the deficiencies discussed in this report are presented in general terms only; specific details of the findings were separately provided to management. Although no quantifiable monetary benefits were disclosed, the audit showed that opportunities existed for improving computer security within the Defense Information Systems Agency (Appendix E). The cumulative results of this audit and two prior followup audits are provided in Appendix D of this report. The results of

this audit of the corrective actions taken by the Defense Information Systems Agency are summarized below and in more detail in Part I of the report.

o Controls over sensitive features of the operating system needed further improvement at the Defense Megacenter, Denver, Colorado. As a result, application programs and data, such as pay records, could be added, modified, or deleted without detection. The lack of control over one operating system feature was a material weakness (Finding A).

o Controls over certain aspects of the security software at the Defense Megacenter, Denver, Colorado, were not adequately implemented. A new security problem related to a sensitive administrative authority was also identified. The Defense megacenters in Denver, Colorado, and St. Louis, Missouri, immediately corrected the new security problem on their systems. However, the Defense Information Systems Agency, Western Hemisphere, Fort Ritchie, Maryland, needed to verify that the same problem did not exist at other Defense megacenters. Because of these weaknesses, knowledgeable users at both Defense megacenters and possibly at other locations could gain unauthorized system access or perform unauthorized tasks without detection. At the Defense Megacenter, Denver, Colorado, the integrity was jeopardized on one computer system used for processing payroll transactions of $29 billion annually. Similar integrity problems may exist at other Defense megacenters if excessive access was granted to the sensitive administrative authority (Finding B).

Summary of Recommendations, Management Comments, and Audit Response. We recommend improvements in the control and oversight of operating system and security software by the Defense Information Systems Agency, Western Hemisphere, and the Defense Megacenter, Denver, Colorado. Implementing the recommendations made in this report will complete the corrective actions required in response to the prior recommendations we evaluated. Management concurred in the findings and recommendations. Pending its replacement, the use of one supervisor call was being monitored. Improvements had been made or were planned in the controls over sensitive utilities, a monitoring facility, and the tape management system. Although concurring with the recommendations, management did not provide adequate comments on Recommendations B.1.b., B.2.a., B.2.b., and B.2.c. We request that management provide additional comments on this report by February 5, 1996. See Part I for our response to management's comments and Part III for the complete text of the comments.

Table of Contents

Part I - Audit Results

Audit Background

Computer Security. During FYs 1990 through 1994, the Inspector General (IG), DoD, and the Air Force Audit Agency (AFAA) performed a series of five audits to evaluate controls over operating system and security software and other general controls for computer systems supporting the Defense Finance and Accounting Service (DFAS). As detailed in Appendix B, the audits determined that financial computer systems critical to DoD were exposed to fraud and other risks. Knowledgeable users could exploit weaknesses in the operating system controls to improperly access, add, modify, or destroy sensitive computer data, programs, and other resources (accidentally or intentionally) without risk of detection.

Congressional and DoD Oversight. Heightened concern over DoD computer security surfaced during FY 1994. As a result, the IG, DoD, was asked to follow up on prior audits of computer security. In April 1994, the Deputy IG testified on DoD financial management issues before the Senate Governmental Affairs Committee. The Deputy IG advised the committee that inadequate controls over computer security were among several high-risk problems requiring the immediate attention of DoD. In May 1994, the committee chairman requested that the IG, DoD, closely monitor DoD efforts to correct weaknesses in computer security and other financial management problems.

Also in April 1994, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) requested a briefing on computer security from the IG, DoD. As a result of that briefing and directions from the Assistant Secretary, the Defense Information Systems Agency (DISA) created a task force on information security (the DISA task force) to improve information systems security at all Defense megacenters, including the computer centers that were being consolidated into DISA Western Hemisphere (WESTHEM) Defense megacenters. One of the DISA task force objectives was reviewing and verifying the implementation of prior audit recommendations related to computer security at those sites.

In June 1994, the Senior Financial Management Oversight Council, chaired by the Deputy Secretary of Defense, was briefed on the computer security of DoD financial management systems. Among other actions, the Deputy Secretary of Defense directed DISA and DFAS to ensure that problems in computer security were corrected. The Deputy Secretary of Defense also expressed reliance on the IG, DoD, to provide oversight to ensure that security was improved.

Audit Request. On July 12, 1994, in response to directions from the Deputy Secretary of Defense, the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) requested that the IG, DoD, confirm that DFAS and DISA had corrected the previously reported problems with computer security. The IG, DoD, expanded the audit scope to include evaluating corrective actions taken by the Defense Megacenter, Denver, Colorado (DMC-Denver) in response to a

prior AFAA report and by the Defense Logistics Agency, Defense Systems Design Center (DLA-DSDC), in response to the prior IG, DoD, report. The prior reports are listed in Appendix B.

Followup Completed. In responding to the audit request, we issued the following reports on the followup completed at DFAS, DISA, and DLA:

o Report No. 95-263, "Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service," June 29, 1995, and

o Report No. 95-270, "Corrective Actions on System and Software Security Deficiencies," June 30, 1995.

The three Defense agencies made commendable efforts to implement the prior audit recommendations. However, corrective action was still required on 20 of the 87 recommendations followed up in those audits. Followup on another 25 recommendations was deferred to the current audit because of the ongoing systems migrations.

Current Followup. This report summarizes the audit of corrective actions performed by DMC-Denver and the Defense Megacenter, St. Louis, Missouri (DMC-St. Louis), in response to recommendations made in the following reports:

o Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992, and

o Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994.

These two reports recommended improvements and additions to security and operating system software controls at the Marine Corps Computer and Telecommunications Activity (MCCTA) and at the DISA WESTHEM Defense Information Processing Centers (DIPCs) at Indianapolis, Indiana, and Kansas City, Missouri. During FY 1995, the computer systems previously audited at MCCTA and DIPC-Kansas City migrated to DMC-St. Louis. The computer system previously audited at DIPC-Indianapolis migrated to DMC-Denver during the same period.

Technical Terms. See Appendix C, "Glossary," for definitions of the technical terms used in this report.

Audit Objectives

The objective of our audit was to determine whether corrective actions taken or planned by DMC-Denver and DMC-St. Louis to improve computer security adequately responded to the recommendations made to MCCTA, DIPC-Indianapolis, and DIPC-Kansas City in IG, DoD, Reports No. 93-002 and 94-065. In addition, we evaluated the effectiveness of applicable management controls.

See Appendix A for a discussion of the scope and methodology and the results of our review of the management control program.

Finding A. Operating Systems

Both DMC-Denver and DMC-St. Louis had significantly improved their operating system controls on the five systems audited. However, DMC-Denver needed to take additional corrective actions on 2 of 16 prior audit recommendations. Specifically, DMC-Denver programmers had not eliminated one supervisor call (SVC) that jeopardized system integrity, nor had they established adequate controls over sensitive utilities on System 615A. This problem occurred because system programmers at DIPC-Indianapolis used an ineffective control technique with the SVC. Also, the programmers incorrectly installed one sensitive utility. Security software controls were not implemented over commands issued for two other sensitive utilities through the monitoring facility. This weakness allowed anyone using that monitoring facility to issue the sensitive utility commands. As a result of these weaknesses, application programs and data, such as pay records, could be added, modified, or deleted without detection, and the system's integrity was jeopardized. The SVC exposure is a material management control weakness.

Operating System Function and Summary of Results

Function of Operating System. As further detailed in the discussion of methodology in Appendix A, the audit focused on the operating systems covered by our prior audits and the Computer Associates, Incorporated, CA-TOP SECRET security software used by those systems, as follows:

o System 615A, which migrated to DMC-Denver from DIPC-Indianapolis,

o Systems TT0B and TT0C, which migrated to DMC-St. Louis from DIPC-Kansas City, and

o Systems GX0A and GG0A, which migrated to DMC-St. Louis from MCCTA.

The operating system is a major component of any computer system. It is an integrated collection of computer programs, service routines, and supervisory procedures that directs the sequence and processing of computer applications (scheduling jobs, loading programs, allocating computer memory, managing files, and controlling input and output operations). The Multiple Virtual Storage (MVS) operating systems also isolate and protect individual user programs. When the operating system features are properly administered and controlled, only authorized programs can modify the processing of other programs. However, operating systems are not intended to guarantee that only authorized users can execute authorized programs. As discussed in Finding B, commercial security software packages control authorized users.

Summary of Results. Prior audits at DIPC-Indianapolis, DIPC-Kansas City, and MCCTA identified computer security problems caused by inadequate controls over SVCs and sensitive utility programs (Appendixes B and D). Some of those management control weaknesses were material.

This followup audit determined that DMC-St. Louis had adequately implemented the nine prior recommendations made to MCCTA and DIPC-Kansas City. However, DMC-Denver needed to take additional action to adequately implement two recommendations made to DIPC-Indianapolis to improve the controls over one SVC and certain sensitive utilities. Details of our findings are presented below and in Appendix D.

Supervisor Calls

Although DMC-Denver took action to control the SVCs on System 615A, one SVC had an integrity exposure. This resulted because system programmers at DIPC-Indianapolis used an ineffective control technique (an imbedded password) to safeguard system integrity. Imbedded passwords were formerly used by the computer industry to control access to SVCs. However, research showed that the passwords could be extracted by knowledgeable users. System programmers at DMC-Denver were aware of the problem with imbedded passwords and had begun reviewing ways to eliminate the integrity exposure. This integrity exposure allowed any knowledgeable user to bypass normal controls on the operating system and security software. Thus, users could add, modify, or delete system data without detection. The integrity exposure caused by this SVC is a material management control weakness.

Sensitive Utilities

On the DMC-Denver System 615A, three sensitive utility programs were not adequately controlled. Commands for two of the three sensitive utilities could be issued through the monitoring facility. Also, the parameters of the third sensitive utility were not properly defined. The inadequate controls existed because system programmers at DIPC-Indianapolis did not correctly install one sensitive utility. Security software controls were not implemented over the issuance of commands for the remaining two utilities through the monitoring facility. Knowledgeable users could execute these utilities to destroy data on tape files, bypass security, or make unauthorized changes to programs or data to which they had access.

Recommendations for Corrective Action

A. We recommend that the Director, Defense Information Systems Agency, Western Hemisphere, Defense Megacenter, Denver, Colorado, take the following corrective actions on System 615A:

1. Make the appropriate changes required to eliminate the integrity exposure on the one supervisor call.

2. Install sensitive utilities so that parameters are properly defined.

3. Implement security software controls over the issuance of sensitive utility commands through the monitoring facility.

Management Comments

Management concurred with Recommendation A.1. to eliminate the integrity exposure caused by one SVC stating that all programs that call the SVC are being monitored. Management planned to replace the SVC in March 1996 with a secured SVC. Management also concurred with Recommendation A.2. stating the parameters on one sensitive utility had been redefined by activating a special option on System 615A. Finally, management concurred with Recommendation A.3. to control the issuance of commands for two sensitive utilities through the monitoring facility. Management stated that the security option had been activated for the monitoring facility so that only authorized users could issue commands for the two utilities. See Part III for the complete text of management's comments.

Finding B. Implementation of Security Software

The DMC-St. Louis and DMC-Denver had significantly improved their security software controls by taking corrective action on five of six prior audit recommendations. DMC-Denver had not fully implemented the remaining recommendation, as follows:

o The tape management system and access authorizations to the production job scheduling system were not adequately controlled.

o Update access to the master catalog was not restricted to the system personnel who maintained it.

These problems existed when System 615A migrated to DMC-Denver from DIPC-Indianapolis. DMC-Denver did not have time to correct the exposures because of all the demands placed on its limited resources by the system migration. In addition, DISA guidelines did not address the tape management system or how to implement new security interface options.

A new security problem with potentially wide impact in DISA WESTHEM was identified. Excessive access had been given to an administrative authority feature of the security software that allowed users to initiate sensitive special attributes. Security officials at the two Defense megacenters were not aware that the assignment of the administrative authority could result in modification of the CA-TOP SECRET control options.

By improper use of CA-TOP SECRET security software, DMC-Denver and DMC-St. Louis increased the risk that knowledgeable users may gain unauthorized access or perform unauthorized tasks without detection. The security weaknesses at DMC-Denver jeopardized the integrity of the system that processes Army active-duty and Reserve payrolls totaling $29 billion annually. Although both Defense megacenters immediately corrected the new security problem on their systems, similar integrity problems may exist at other Defense megacenters if excessive access has been granted to the administrative authority.

Security Software Function and Summary of Results

Function of Security Software. Security software is used to protect computer resources such as files, programs, tapes, database definitions, libraries, readers, and processing capabilities. As stated in Finding A, the audit focused on the computer operating systems covered by our prior audits and the CA-TOP

SECRET security software used by those systems, currently identified as follows:

- o System 615A at DMC-Denver, and
- o Systems TT0B, TT0C, GX0A, and GG0A at DMC-St. Louis.

CA-TOP SECRET security software offers a variety of control options and features to enhance system security. The control options and features of the security software should be set for the level of security needed. The level of protection achieved depends on how well the options and features of CA-TOP SECRET are administered.

Summary of Results. In prior audits, the IG, DoD, identified computer security problems at DIPC-Indianapolis, DIPC-Kansas City, and MCCTA. The problems were caused by inadequate controls over security software (Appendixes B and D). Some of these management control weaknesses were material in nature.

Despite the significant strides made by DMC-Denver and DMC-St. Louis in improving controls over security software, this followup audit determined that additional corrective actions by DMC-Denver were required to fully implement one recommendation. The audit also identified a new computer security problem related to an administrative authority. This problem may exist at other DISA WESTHEM organizations, as discussed below. Details of our findings are presented below and in Appendix D.

Tape Management System

DMC-Denver had not adequately secured tape file processing on System 615A. DMC-Denver used the Computer Associates, Incorporated, CA-1 Tape Management System to manage the movement of tapes and cartridges. The new product version of CA-1 includes 10 security interface options that provide additional protection beyond CA-1 password protection by an interface to CA-TOP SECRET. These security interface options include dataset name protection during open and end-of-volume processing, protection for the creation of secondary data sets, on-line interfaces, and CA-1 batch updates. Examples of other options include label processing, on-line commands, and EXPDT=98000 processing (the CA-TOP SECRET feature that restricts the bypassing of tape management system checks). To invoke the security interface options, DMC-Denver personnel must activate each of these options separately. These options were not activated on System 615A because DISA guidelines did not address the CA-1 Tape Management System or implementation of the product's new security interface options. Unless these security interface options are activated, CA-TOP SECRET security checks are not accomplished and this additional protection is not provided.

Production Job Scheduling System

Production scheduling is a process used to schedule and start specific jobs. The production job scheduling system at DMC-Denver allowed greater authority to submit jobs, without job security checking and auditing, than should be allowed to accomplish production scheduling. In addition, DIPC-Indianapolis had established user accessor identifiers (ACIDs) that were shared by more than one user. No individual can be held accountable for the functions performed when shared ACIDs are used. DMC-Denver was aware of this exposure. However, management did not have sufficient time to address this problem along with the other demands placed on its limited resources by the system migration. Without adequate controls over production scheduling, the integrity of the system that processes Army active-duty and Reserve payrolls totaling $29 billion annually was not ensured.

Master Catalog

The master catalog is a critical file with an index containing extensive file and volume information. The computer's operating system uses this information to locate files, create and delete storage space, verify program or operator authorization to access a file, and accumulate usage statistics. If the master catalog is disabled, accidentally or deliberately, the operating system will not function.

DIPC-Indianapolis did not restrict update access to the master catalog to the system programmers who maintain it. For example, 4 ACIDs were assigned to profiles (see Appendix C, "Glossary") that gave 72 users update access to the master catalog. Only the system programmers who maintain the master catalog should have update access.

DMC-Denver recognized the need to evaluate and strengthen access controls to the master catalog. This task was extensive because implementation procedures, standards, and security rules had to be reviewed. The DMC-Denver did not have sufficient time to complete the task since the system's migration from DIPC-Indianapolis. DMC-Denver managers expected to complete the task by December 31, 1995.

Administrative Authority

A new security problem was identified with potentially wide impact in DISA WESTHEM. The DIPC-Indianapolis, DIPC-Kansas City, and MCCTA had given excessive access to an administrative authority feature that allowed users to initiate sensitive special attributes. For example, the use of this feature

allowed access to the CONSOLE attribute, a sensitive restricted attribute that gives users the ability to change CA-TOP SECRET control options. At the time of our audit, 15 users on the DMC-Denver system and 26 users on the DMC-St. Louis systems could use the administrative authority to assign specific special attributes to themselves. Of the 41 total users, 28 (6 at DMC-Denver and 22 at DMC-St. Louis) should not have had the unlimited access allowed by the administrative authority. Security officials at both Defense megacenters were not aware that this administrative authority could be used to modify the CA-TOP SECRET control options.

When managers at DMC-Denver and DMC-St. Louis were notified of this condition, they took immediate action to control the use of the administrative authority. The administrative authority granted to the 28 users was redefined to reduce the risk of unauthorized changes being made to the CA-TOP SECRET security software. We did not make recommendations in this report to DMC-St. Louis and DMC-Denver because of their prompt corrective action on this issue. However, based on our findings at those two organizations, we advised the DISA WESTHEM Security Office of our concern that the same problem may exist at other Defense megacenters.

Recommendations for Corrective Action

B.1. We recommend that the Commander, Defense Information Systems Agency, Western Hemisphere:

a. Amend the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards" to include standard guidelines for implementation of the Computer Associates, Incorporated, CA-1 Tape Management System.

b. Amend the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards" to address the sensitive administrative authority and restrict its use to authorized security administrators.

c. Include in the Defense Information Systems Agency, Western Hemisphere, security compliance inspections a review of the Defense megacenters' implementation of the Computer Associates, Incorporated, CA-1 Tape Management System and the use of the sensitive administrative authority, as established in accordance with Recommendations B.1.a. and B.1.b.

B.2. We recommend that the Director, Defense Megacenter, Denver, Colorado, direct the following actions for System 615A:

a. Implement the Production Job Scheduling System to allow for job security checking and auditing.

b. Define all users individually to the system by assigning user accessor identifiers according to the users' needs, and remove all shared accessor identifiers.

c. Limit access to update the master catalog to the system programmers responsible for maintaining the master catalog.

Management Comments

Management concurred with Recommendation B.1.a. stating that the next revision to the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards" (scheduled for March 1996) would include controls for the tape management system. Management also concurred with Recommendation B.1.c. stating that the current checklist used in conducting DISA WESTHEM security compliance inspections provides for a review of the controls over the tape management system. By December 1995, management plans to revise the checklist to include a review of the use of the sensitive administrative authority.

Management concurred with Recommendations B.2.a. through B.2.c. to improve controls over the Production Job Scheduling System, accessor identifiers, and the master catalog. However, the comments provided by management actually related to Recommendations B.1.a. and B.1.c. to improve controls over the CA-1 Tape Management System. See Part III for the complete text of management's comments.

Audit Response

Management's comments on Recommendations B.1.a. and B.1.c. were fully responsive. However, no management comments were provided for the other recommendations, as discussed below:

o Management did not comment on Recommendation B.1.b. to revise the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards" to provide guidance on the sensitive administrative authority.

o Although, management comments were provided for Recommendations B.2.a. through B.2.c., they actually related to Recommendations B.1.a. and B.1.c., which concern the CA-1 Tape Management System.

In accordance with DoD Directive 7650.3, additional comments are requested from DISA on Recommendations B.1.b., B.2.a., B.2.b., and B.2.c.

Part II - Additional Information

Appendix A. Scope and Methodology

Scope and Methodology

Methodology. We examined operating system features that can affect the integrity of operating system and security software. Those operating system features were the authorized program facility (APF), SVCs, the time share option, the program properties table (PPT), the job entry subsystem 2 (JES2), started tasks, and sensitive utilities. We examined the implementation of the CA-TOP SECRET security software. We also examined other general controls over sensitive programmer positions, the tape management system, and the off-site storage of operating system backups.

The audit was limited to evaluating the controls over the computer systems covered by our prior audits. At DMC-Denver, the audit was limited to evaluating the controls over System 615A. This was the DIPC-Indianapolis computer system identified in our Report No. 93-002 that processed the Army Joint Uniform Military Pay System. We did not follow up on the prior recommendations made in Report No. 93-002 on the test system at DIPC-Indianapolis. That system was being merged with other DMC-Denver systems and was not expected to exist after December 31, 1995. At DMC-St. Louis, the audit was limited to evaluating the controls over four computer systems:

o Systems TT0B and TT0C (previously identified in Report No. 94-065 as the Defense Information Services Organization-Kansas City systems), and

o Systems GX0A and GG0A (previously identified in Report No. 94-065 as the MCCTA Worldwide Support Division system and the MCCTA system, respectively).

Use of Computer-Processed Data. To achieve the audit objectives, we relied on computer-processed data in the operating system libraries and the security software of each organization. We used the Computer Associates, Incorporated, CA-EXAMINE audit software to extract data directly from computer memory and operating system libraries. The CA-EXAMINE software audits MVS operating systems. We used automated and manual techniques to analyze system data. For example, to test operating system and security rules and features, we used the audit features of the CA-TOP SECRET security software. All system testing and use of audit software were done in a controlled environment with management's approval. Based on those tests and assessments, we concluded that the data were sufficiently reliable to be used in meeting the audit objectives.

Organizations Visited, Audit Period, and Standards. We performed audit work at DMC-Denver and DMC-St. Louis. This program audit was performed from April 4 through July 14, 1995. The audit was made in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the IG, DoD, and accordingly included such tests of

management controls as were considered necessary. During the audit, we visited or contacted the organizations shown in Appendix F.

Management Control Program

DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended, and to evaluate the adequacy of the controls.

Scope of Review of Management Control Program. We reviewed the adequacy of management controls over sensitive features of the operating system and security software and other general controls at DMC-Denver and DMC-St. Louis. We did not evaluate the implementation of the DoD management control program at these two Defense megacenters because a recent audit determined that DISA WESTHEM had improperly defined its assessable units in FY 1994.* The DISA WESTHEM treated the 16 Defense megacenters as a single assessable unit (computer operations) during FY 1994. Doing so was not reasonable because these Defense megacenters represented the majority of the mission and resources of DISA WESTHEM. To correct this problem, DISA WESTHEM designated each Defense megacenter as an assessable unit during FY 1995. We also did not evaluate the management control program at MCCTA because no audit work was performed at that organization.

Adequacy of Management Controls. The followup audit at the two Defense megacenters evaluated management controls over the operating system and security software and other general controls. Material management control weaknesses, as defined by Office of Management and Budget Circular No. A-123 and DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987, existed in DMC-Denver's general controls over one SVC. Inadequate controls over this sensitive feature of the operating system made it possible for knowledgeable users to improperly access, modify, or destroy sensitive computer data and programs without detection. Implementing Recommendation A.1. will correct the material weakness in SVC controls on the operating system at DMC-Denver. See Part I (Finding A) of this report for details. As shown in Appendix E, strengthened management controls and other nonmonetary benefits will be realized from implementing the recommendations. A copy of the report will be provided to the senior official in DISA responsible for management controls.

*The audit of the DISA WESTHEM management control program was discussed in IG, DoD, Report No. 95-280, "Internal Management Control Program, Defense Information Systems Agency, Western Hemisphere," July 26, 1995.

Appendix B. Summary of Prior Audits and Other Reviews

Computer Security Audits

Prior IG, DoD, and AFAA audits determined that financial computer systems critical to DoD were exposed to fraud and other risks. Knowledgeable users could exploit weaknesses in the operating system and security software and other general controls to improperly access, add, modify, or destroy sensitive computer data, programs, and other resources (accidentally or intentionally) without risk of detection. Management generally concurred in the recommendations made to improve computer security. The reports issued on these prior audits and the audit followup made in this and other IG, DoD, audits are discussed below.

AFAA Report, "Data Processing Center (DPC) Operations and Security at the Air Force Accounting and Finance Center (AFAFC) (Project No. 0195410)," August 5, 1991. The report identified weaknesses in the controls over operating system and security software at the finance center. IG, DoD, Report No. 95-263, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 29, 1995, was issued on the followup made on the prior recommendations, which were intended to improve the security of the computer center (now DMC-Denver) of the Air Force Accounting and Finance Center.

IG, DoD, Report No. 93-002, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," October 2, 1992. The report identified weaknesses in the controls over the operating system and security software at two DISA organizations: DIPC-Cleveland and DIPC-Indianapolis. IG, DoD, Report No. 95-263 was issued on the followup at DIPC-Cleveland. See Part I of this report for a discussion of the followup results at DMC-Denver on the recommendations made to DIPC-Indianapolis. Repeat findings at DMC-Denver were reported in Finding A on sensitive features of the operating system and in Finding B on the tape management system, the production scheduling system, and the master catalog.

IG, DoD, Report No. 93-133, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," June 30, 1993. The report identified weaknesses at DIPC-Dayton, DIPC-Columbus (now DMC-Columbus), and the DLA Defense Systems Automation Center (now DLA-DSDC) over operating system and security software. The DIPC-Dayton no longer exists because its work load migrated to DMC-Columbus during FY 1994. IG, DoD, Report No. 95-263 was issued on the followup at DLA-DSDC and DMC-Columbus.

IG, DoD, Report No. 94-060, "General Controls for Computer Systems at the Information Processing Centers of the Defense Information Services Organization," March 18, 1994. The report identified weaknesses at one DFAS and three DISA organizations in controls over abnormal endings to computer operations; maintenance and security oversight of automatic data processing equipment; access to sensitive computer assets; and potential environmental hazards. Weaknesses in change control procedures at the DFAS Financial Systems Activity (FSA) Denver were also identified. See IG, DoD, Report No. 95-270, "Corrective Actions on System and Software Security Deficiencies," June 30, 1995, for followup at DFAS FSA Denver. See IG, DoD, Report No. 95-263 for followup at the Defense Information Services Organization (now DISA WESTHEM), DIPC-Columbus (now DMC-Columbus), and DIPC-Denver (now DMC-Denver). We determined that followup was no longer viable on recommendations to DIPC-Indianapolis to make structural improvements or revise operating procedures. Such recommendations were made obsolete when the DIPC-Indianapolis computer system migrated to DMC-Denver.

IG, DoD, Report No. 94-065, "Controls Over Operating System and Security Software Supporting the Defense Finance and Accounting Service," March 24, 1994. The report identified weaknesses in the controls over operating system and security software at DFAS FSA Pensacola (now DIPC-Pensacola), DIPC-Kansas City, MCCTA, and MCCTA Worldwide Support Division. See IG, DoD, Report No. 95-270 for followup at DIPC-Pensacola. The computer systems previously audited at DIPC-Kansas City and both Marine Corps organizations migrated to DMC-St. Louis during FY 1995. See Part I of this report for a discussion of followup at DMC-St. Louis on the recommendations made to DIPC-Kansas City and the two Marine Corps organizations.

IG, DoD, Report No. 95-066, "Controls Over Application Software Supporting the Navy's Inventories Held for Sale (Net)," December 30, 1994. The report identified weaknesses in the controls over operating system and security software, and in the integrated data management system at DMC-Mechanicsburg (Pennsylvania) and the Naval Supply Systems Command, Ships Parts Control Center, Mechanicsburg, Pennsylvania. The prior report had not been issued at the time this followup audit was requested. Followup on the 11 recommendations made in IG, DoD, Report No. 95-066 will be performed under a separate audit.

Audit Followup

Except for IG, DoD, Report No. 95-066, followup was conducted on the prior audits under the present audit and two other followup audits. IG, DoD, Reports No. 95-263 and 95-270 were issued on the other followup audits.

The earlier followup audits determined that DFAS, DISA, and DLA made commendable efforts to implement prior audit recommendations. However, the

3 Defense agencies had not adequately implemented 20 of 87 prior audit recommendations. The reports identified weaknesses in the controls over operating system and security software, environmental hazards, system recertification reviews, change controls, and other operating procedures. Certain weaknesses in the operating system were considered material. Improvements were recommended in operating system and security software, environmental controls, and management controls.

Appendix C. Glossary

Access Control is a general term used to describe a number of techniques that restrict users of a computer system from gaining access to the system or each others' data, or from performing unauthorized actions. When applied to software, access control usually refers to one of the specialized software security packages, such as CA-TOP SECRET.

Accessor Identifier (ACID) is a method by which users sign on to a computer and are identified. This term is used for CA-TOP SECRET security software.

Application Programs are programs that are intended to serve particular business or nonbusiness needs and have specific input, processing, and output activities. Accounts receivable, general ledger, payroll, and personnel programs are examples of application programs.

Authorized Program Facility (APF) is an International Business Machines Corporation (IBM) mechanism for protecting the integrity and security of the MVS operating system. It provides for the orderly, controlled extension of the operating system by defining special program libraries that may contain programs that are authorized to execute in the supervisor state. APF-authorized programs have the potential to bypass all security controls.

Only properly authorized programs should be allowed to perform sensitive tasks such as accessing or modifying another program's execution or data areas. A program that can perform sensitive functions outside of established APF rules can become part of the operating system, and can circumvent or disable all security mechanisms, alter audit trails, or modify any computerized data, regardless of the presence of access control software.

According to the IBM security manual for MVS operating systems, APF procedures should require system programmers to use security software to control the creation of and access to APF libraries and the creation of APF programs. All APF programs should have unique names to prevent mix-ups in processing, and the file containing the names of APF libraries and volume serial numbers (disk device numbers) should reflect only valid libraries and volume serial numbers. Failure to comply with these IBM guidelines can introduce significant integrity exposures to the operating system, and can lessen management's control over system software.

Data base is a collection of interrelated data stored together.

Disk is a data storage device that allows data to be accessed randomly or sequentially without passing through unwanted data.

File is a collection of related data records stored on an external storage medium, usually a disk or tape.

Imbedded Passwords are passwords that are coded into a program.

Job is a basic unit of work on an IBM computer. A job consists of one or more steps or program executions.

Job Control Language is a problem-oriented computer language used in a job that identifies the job or describes its requirements to the operating system.

Job Entry Subsystem 2 (JES2) is one of two IBM job management routines that reads the job stream and assigns jobs to class queues (computer data or programs awaiting processing). The other job management routine is JES3. JES2 processes jobs and manages system input and output processing. JES2 parameters control how and with what restrictions jobs will be run on a computer system.

JES2 options allow console operator commands to be placed in job control language. The options are assigned by type of job class. There are 36 possible batch job classes, and two additional special classes for time-share-option logons and started tasks.

Multiple Virtual Storage (MVS) is the IBM multiple virtual storage operating system.

Profile is a CA-TOP SECRET term related to security administration. Profile user identifications contain permissions and access levels to resources for multiple users; their purpose is to provide a place in the security data base where common access to resources can be stored.

Program Properties Table (PPT) contains the names of special programs, including their codes and properties. Some MVS programs are allowed extraordinary powers and privileges not normally permitted by the operating system. A list of these programs, including their special powers and privileges, is maintained in MVS, and is known as the PPT.

Programs in the PPT can bypass security software mechanisms such as password protection, can ignore file integrity, and can assign a unique storage protection key of less than eight. All of these events are potential threats to system integrity. It is important to ensure that all programs in the PPT have only the capabilities needed to function properly, and that the programs are safeguarded against unauthorized use.

Program names must be kept in a special library created and controlled by the installation, or in two IBM default libraries. The program must also be contained in an APF-authorized library. Controls are intact if users cannot get a Trojan Horse program into an APF-authorized library by using the name of a nonexistent program. However, if APF controls are weak, the risk of unauthorized entry increases.

Sensitive Utilities are utility programs (as defined below) that can bypass system security software or management controls and destroy data if not used properly.

Software is a generic term used to define all programming on a computer system, whether supplied by vendors or developed by in-house programmers. System software includes the operating system and accompanying utility programs that enable a user to control, configure, and maintain the computer system software.

Supervisor Call (SVC) is an assembler language instruction that causes a hardware interruption when executed. The operating system then passes control to the SVC to tell the operating system what service is being requested (open a file for read or write access, close a file, etc.).

SVCs are divided into two categories. One category is available to all programs, while the second is restricted to APF-authorized programs only. Validity checking is the control technique that limits the execution of sensitive, unrestricted SVCs. The first 200 SVCs are provided by IBM or other software vendors. The remaining 56 SVCs can be added by a computer center's in-house programmers to meet its unique requirements or vendor software requirements.

Trojan Horse is a program that executes under an assumed identity or name. It uses a normal program name, but performs unauthorized tasks not associated with the normal program name. For example, in a payroll system, a Trojan Horse program could be used to give employees unauthorized promotions or pay increases.

Update Access is a feature of the security system that allows write access to a file.

Utility Programs are computer programs or routines that perform general data- and system-related functions required by other application software, by the operating system, or by users. Examples include copying, sorting, and merging files.

Appendix D. Summary of Current and Previous Followup Audit Results by Finding, Report, Recommendation, and Responsible Organization as of July 14, 1995

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action Adequate[3] Closed	Adequate[3] Open	Additional Required	Total
Finding A. Operating Systems							
93-002	A.2.a.	APF	DIPC-Indianapolis	1	0	0	1
93-002	A.2.b.	APF	DIPC-Indianapolis	1	0	0	1
93-002	A.2.c.	APF	DIPC-Indianapolis	1	0	0	1
93-002	A.2.d.	PPT	DIPC-Indianapolis	1	0	0	1
93-002	A.2.e.	JES2	DIPC-Indianapolis	1	0	0	1
93-002	A.4.a.	Supervisor Calls	DIPC-Indianapolis	0	1	0	1
93-002	A.4.b.	Utilities	DIPC-Indianapolis	0	1	0	1
94-065	A.1.a.	Guidelines	MCCTA	1	0	0	1
94-065	A.1.b.(1)	APF	MCCTA	1	0	0	1
94-065	A.1.b.(2)	APF	MCCTA	1	0	0	1
94-065	A.1.b.(3)	PPT	MCCTA	1	0	0	1
94-065	A.1.b.(4)	JES2	MCCTA	1	0	0	1
94-065	A.1.b.(5)	Utilities	MCCTA	1	0	0	1
94-065	A.2.a.	Guidelines	DIPC-Kansas City	1	0	0	1
94-065	A.2.b.(1)	APF	DIPC-Kansas City	1	0	0	1
94-065	A.2.b.(3)	Utilities	DIPC-Kansas City	1	0	0	1
Subtotal, Finding A			(a)	**14**	**2**	**0**	**16**
Summary by Responsible Organization, Finding A[4]							
DMC-Denver				5	2	0	7
DMC-St. Louis				9	0	0	9

Note: See the footnotes at the end of the appendix.

Appendix D. Summary of Audit Results by Finding, Report, Recommendation, and Organization

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action: Adequate[3]: Closed	Adequate[3]: Open	Additional Required	Total
Finding B. Security Software and Environmental Controls							
93-002	C.2.	Security Software	DIPC-Indianapolis	0	1	0	1
94-065	B.1.a.	Security Software	DIPC-Kansas City	1	0	0	1
94-065	B.1.b.	Security Software	DIPC-Kansas City	1	0	0	1
94-065	B.1.c.	Security Software	DIPC-Kansas City	1	0	0	1
94-065	B.2.a.	Security Software	MCCTA	1	0	0	1
94-065	B.2.b.	Security Software	MCCTA	1	0	0	1
Subtotal, Finding B			(b)	5	1	0	6
Summary by Responsible Organization, Finding B[4]							
DMC-Denver				0	1	0	1
DMC-St. Louis				5	0	0	5
Other General Controls							
94-065	C.1.a.	System Programmer	MCCTA	1	0	0	1
94-065	C.1.b.	Tape Management System	MCCTA	1	0	0	1
94-065	C.1.c.	Off-Site Storage	MCCTA	1	0	0	1
Subtotal, Other General Controls			(c)	3	0	0	3
Summary by Responsible Organization, Other General Controls[4]							
DMC-Denver				0	0	0	0
DMC-St. Louis				3	0	0	3
Subtotal, Current Followup Audit Findings			(d) = (a+b+c)	22	3	0	25
Summary by Responsible Organization - Current Followup Audit Findings[4]							
DMC-Denver				5	3	0	8
DMC-St. Louis				17	0	0	17

Note: See the footnotes at the end of the appendix.

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action Adequate: Closed	Adequate: Open	Additional Required	Total
Results of Prior Followup Audits							
95-263	Various	Various	DMC-Denver	24	0	3	27
95-263	Various	Various	DMC-St. Louis	0	0	0	0
95-263	Various	Various	DISA WESTHEM-Other	21	5	10	36
95-263	Various	Various	DLA-DSDC	14	0	2	16
95-270	Various	Various	DFAS FSA Denver	3	0	0	3
95-270	Various	Various	DISA WESTHEM-Other	5	0	0	5
Subtotal, Results of Prior Followup Audits			(e)	67	5	15	87
Summary by Responsible Organization - Results of Prior Followup Audits[4]							
DISA WESTHEM:							
DMC-Denver				24	0	3	27
DMC-St. Louis				0	0	0	0
Other				26	5	10	41
Subtotal, DISA WESTHEM				50	5	13	68
DFAS FSA Denver				3	0	0	3
DLA-DSDC				14	0	2	16
Subtotal, Results of Prior Followup Audits				67	5	15	87
Total, All Recommendations			(f) = (d+e)	89	8	15	112

Note: See the footnotes at the end of the appendix.

Report	Recommendation	Subject Area[1]	Organization[2]	Recommendations Subject to Audit Followup: Corrective Action: Adequate[3]: Closed	Adequate[3]: Open	Additional Required	Total
Summary by Responsible Organization, Grand Total, All Recommendations[4]							
DISA WESTHEM:							
DMC-Denver				29	3	3	35
DMC-St. Louis				17	0	0	17
Other				26	5	10	41
Subtotal, DISA WESTHEM				72	8	13	93
DFAS FSA Denver				3	0	0	3
DLA-DSDC				14	0	2	16
Total, All Recommendations				89	8	15	112

[1]APF=Authorized Program Facility; Guidelines=Operating system installation integrity guidelines; JES2=Job Entry Subsystem 2 parameters; PPT=Program Property Tables; System programmer=Sensitive system programmer positions; and Utilities=Sensitive utilities.

[2]Acronyms used for each organization are defined as follows: DMC-Denver is used for the Defense Megacenter in Denver, Colorado; HQ, DISA WESTHEM is used for the Headquarters, Defense Information Systems Agency, Western Hemisphere, Fort Ritchie, Maryland; DIPC-Indianapolis and DIPC-Kansas City are used for the DISA WESTHEM Defense information processing centers in those cities. DLA-DSDC is used for the Defense Logistics Agency, Defense Systems Design Center, in Columbus, Ohio; and MCCTA is used for the Marine Corps Computer and Telecommunications Activity in Quantico, Virginia.

[3]Closed recommendations represent those recommendations on which the recommended corrective actions (or suitable alternatives) have been completed. Therefore, no additional followup under DoD Directive 7650.3 by the Office of the Assistant Inspector General for Analysis and Followup was planned on closed recommendations. Open recommendations represent those recommendations where the actual corrective actions completed and planned are considered adequate. Followup under DoD Directive 7650.3 is required on open recommendations to verify that planned corrective actions are completed.

[4]DMC-Denver was responsible for acting on the recommendations made in IG, DoD, Report No. 93-002 to DIPC-Indianapolis. The DMC-St. Louis was responsible for acting on the recommendations made in IG, DoD, Report No. 94-065 to DIPC-Kansas City and MCCTA.

Appendix E. Summary of Potential Benefits Resulting From Audit

Recommendation Reference	Description of Benefit	Amount and Type of Benefit
A.1., A.2., A.3.	Management controls. Reduces risk of computer fraud by strengthening controls over sensitive features of the operating system on System 615A at DMC-Denver.	Nonmonetary.
B.1.a., B.1.b., B.1.c.	Management controls. Reduces risk of computer fraud within DMC-Denver and other DISA WESTHEM organizations by providing guidance and management oversight of the tape management system and a sensitive administrative authority.	Nonmonetary.
B.2.a., B.2.b., B.2.c.	Management controls. Reduces the risk of computer fraud on System 615A at DMC-Denver by enhancing security over the production job scheduling system, establishing individual user accountability, and controlling update access to the master catalog.	Nonmonetary.

Appendix F. Organizations Visited or Contacted

Department of the Navy

Marine Corps Computer and Telecommunications Activity, Quantico, VA

Other Defense Organizations

Financial Systems Activity, Defense Finance and Accounting Service,
Kansas City, MO
Defense Information Systems Agency, Western Hemisphere, Fort Ritchie, MD[1]
Defense Megacenter, Denver, CO[2]
Defense Megacenter, St. Louis, MO[3]
Kansas City Detachment, Kansas City, MO
Quantico Detachment, Quantico, VA

[1]DISA WESTHEM was referred to in IG, DoD, Reports No. 93-002 and No. 94-065 as either the Defense Information Technology Services Organization or the DISA Defense Information Services Organization.

[2]In IG, DoD, Report No. 94-065, DMC-Denver was referred to as the Defense Information Services Organization's Information Processing Center-Denver. The DMC-Denver was responsible for acting on the recommendations made to DIPC-Indianapolis in IG, DoD, Report No. 93-002.

[3]DMC-St. Louis was responsible for acting on the recommendations made to DIPC-Kansas City and MCCTA in IG, DoD, Report 94-065.

Appendix G. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)*
  Deputy Chief Financial Officer
    Director, Chief Financial Officer Support Office
      Chief, Internal Management Control Division
      Internal Control Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)*
Director, Defense Logistics Studies Information Exchange
Assistant to the Secretary of Defense (Public Affairs)
Internal Control Officer, Directorate for Organizational and Management Planning, Administration and Management

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Policy Liaison Division, Office of the Assistant Director, Policy and Plans, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service Denver Center

*Recipient of draft report.

Chief, Audit Control and Liaison, Customer Service and Performance Assessment
Deputate, Defense Finance and Accounting Service
Director, Defense Information Systems Agency*
Commander, Defense Information Systems Agency, Western Hemisphere*
Commanding Officer, Defense Megacenter-St. Louis*
Director, Defense Megacenter-Denver*
Inspector General, Defense Information Systems Agency*
Internal Control Officer, Office of the Comptroller
Chief, Internal Review Group, Office of the Director, Defense Logistics Agency
Inspector General, National Security Agency
Audit and Internal Management Control Liaison, National Security Agency

Non-Defense Federal Organizations and Individuals

Special Projects Branch, National Security Division, National Security and International Affairs, Office of Management and Budget
Information Management and Technology Division, General Accounting Office
Technical Information Center, National Security and International Affairs Division, General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice, Committee on Government Reform and Oversight
House Committee on National Security

*Recipient of draft report.

This page was left out of orignial document

Part III - Management Comments

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURT HOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

Inspector General

22 NOV 1995

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ATTN: DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE

SUBJECT: Draft Audit Report on the Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service (Project No. 5FD-5026)

Reference: DODIG Draft Audit Report, subject as above, 14 Sep 95

1. We have reviewed the subject draft report and concur with the recommendations addressed to DISA. Our management comments are enclosed which discuss corrective actions to be taken on the recommendations. Where corrective action has already been taken, we have identified the actions taken.

2. The point of contact is Ms. Sandra J. Leicht, Audit Liaison. If you have questions on our response, Ms. Leicht can be reached on 703-607-6316.

FOR THE DIRECTOR:

Enclosure a/s

RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

MANAGEMENT COMMENTS TO DODIG FOLLOWUP AUDIT ON CONTROLS OVER OPERATING SYSTEM AND SECURITY SOFTWARE AND OTHER GENERAL CONTROLS FOR COMPUTER SYSTEMS SUPPORTING THE DEFENSE FINANCE AND ACCOUNTING SERVICE PROJECT NO. 5FD-5026

Recommendation A. Recommend that the Director, Defense Megacenter Denver take the following corrective actions on System 615A:

1. Make the appropriate changes required to eliminate the integrity exposure on the one supervisor call.

2. Install sensitive utilities so that parameters are properly defined.

3. Implement security software controls over the issuance of sensitive utility commands through the monitoring facility.

Response to Supervisor Calls (SVCs). Concur with the recommendation. On the migrated system 615A from Indianapolis, DMC Denver reconciled vendor modifications to the IBM SVCs and user/vendor SVCs to letters of system integrity from the various vendors. However, DMC Denver found one user/vendor supervisor call that must be controlled because it could be used to damage or allow unauthorized access to DMC Denver System 615A. The SVC is a totally adapted SVC which is used in the Defense Joint Military Pay System (DJMS) subroutine that call the SVC to effect dynamic changes to dataset names. This SVC is also used on DMC Denver's SYS2 and SYS3.

DMC Denver is currently auditing all programs which call this SVC. It is felt that 99% of all programs that use this SVC have been identified. DMC Denver has begun testing a new secured SVC to replace the existing SVC. The estimated date for implementation in production is March 1996.

Response to Sensitive Utility Programs and Security Software Controls. Concur with the recommendation. On System 615A, the *[A] utilities should be controlled. Since *[A] bypasses standard operating system controls, DMC Denver must activate the options appropriate for its environment. The *[B] option was not activated for System 615A. In addition,

*Deleted or modified sensitive data.

the *[C] and *[D] utilities were not adequately controlled on the DMC Denver System 615A by the security software because their commands could be issued through the * * monitoring facility * .

DMC Denver has turned on the *[B] option on *[A]. DMC Denver has also turned on the security option for the *[monitoring] Facility so that only those system programmers and operators which need the ability to issue privileged commands have that ability. All other users only have the ability display and manage their individual jobs and print output.

Recommendation B.1. Recommend the Commander, DISA WESTHEM:

a. Amend the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards" to include guidelines for implementation of the Computer Associates, Incorporated, CA-1 Tape Management System.

b. Amend the "DISA WESTHEM Personnel and Security: MVS Security Technical Implementation Standards" to address the sensitive administrative authority and restrict its use to authorized security administrators.

c. Include in the DISA WESTHEM security compliance inspections a review of the Defense megacenter's implementation of the Computer Associates, Incorporated, CA-1 Tape Management System and the use of the sensitive administrative authority, as established in accordance with Recommendations B.1.a. and B.1.b.

Response to Recommendation B.1. Concur with the recommendation. The Director of Security, DISA WESTHEM, has initiated action to incorporate standard Tape Management System controls into the MVS TIS. These standards are projected to be included in the next scheduled release of the MVS TIS. The estimated date for this release is projected by March 1996.

The DISA WESTHEM Security Readiness Review (SRR) procedures currently provide checklists for review of the Tape Management Systems and associated controls. However, the checklists do not currently include review of the "administrative" authority. The Director of Security, DISA WESTHEM, will rewrite SRR checklists to include review of this privilege in the next production of the SRR checklist scheduled for release by December 1995.

*Deleted or modified sensitive data.

Recommendation B.2. Recommend that the Director, DMC Denver, direct the following actions for System 615A:

a. Implement the Production Job Scheduling System to allow for job security checking and auditing.

b. Define all users individually to the system by assigning user accessor identifiers according to the users' needs, and remove all shared accessor identifiers.

c. Limit access to update the master catalog to the system programmers responsible for maintaining the master catalog.

Response to Recommendation B.2. Concur with the recommendation. Security interface options for the CA-1 Tape Management Software were not implemented on System 615A. The CA-1 security program called *[E] is designed to interface with CA-Top Secret by creating a security call based on resource class, resource entity, and level of access. Based on the return code from the external security system, *[E] sets the appropriate return code for CA-1 to either allow or disallow access. In order to provide for external security processing, each of the 10 security interface options can be activated or deactivated individually using the associated parameters in *[F] , member *[G]. Unless the options are activated, no calls are made to CA-Top Secret for security checking; therefore, security is not invoked.

DMC Denver will be implementing a new version of CA-1 Tape Management system in November 1995. DMC Denver will at that time invoke the *[E] module and begin implementing and testing the various options of *[E] The estimated date that *[E] security options should be completely implemented is 31 January 1996.

*Deleted or modified sensitive data.

Audit Team Members

This report was prepared by the Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD.

F. Jay Lane
David C. Funk
W. Andy Cooley
Thomas G. Hare
Frances E. Cain
Phillip L. Holbrook, Jr.
Donna L. Meroney
Susanne Allen
Stephanie Price

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Followup Audit of Controls Over Operating System and Security Software and Other General Controls for Computer Systems Supporting the Defense Finance and Accounting Service

B. DATE Report Downloaded From the Internet: 12/08/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 12/08/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.